

Page 17, line 26, delete "fro" and insert therefor
--from--.

IN THE CLAIMS:

Please cancel claims 4, 17, 42-46, 50, 63, 88-107,

add new claims 117-134, and amend the claims as follows:

1. (Amended) A method for inserting a digital signature into digital data, the digital data comprising bits, the method comprising the steps of:

assigning predetermined bits of the digital data for receiving the digital signature;

inserting associated data into the digital data;

signing the digital data excluding the predetermined bits resulting in the digital signature; and

inserting the digital signature into the predetermined bits of the digital data for subsequent authentication of the digital data and the associated data;[.]

wherein at least a portion of the associated data comprises data identifying a public key needed to decrypt the digital signature.

Claims 5, 6, 11, 18, 19, 21, 22, 25, 30, 33, and 38,

line 1, delete "4" and insert therefor --1--.

47. (Amended) An encoder for inserting a digital signature into digital data, the digital data comprising bits, the encoder comprising:

means for assigning predetermined bits of the digital data for receiving the digital signature;

means for signing the digital data excluding the predetermined bits resulting in the digital signature; [and]

means for inserting the digital signature into the predetermined bits of the digital data for subsequent authentication of the digital data[.]; and

means for inserting associated data into the digital data prior to signing the digital data such that the encoder authenticates both the associated data as well as the digital data;

wherein at least a portion of the associated data comprises data identifying a public key needed to decrypt the digital signature.

Claims 51, 52, 57, 64, 65, 67, 68, 76, 79, 80 and 84,
line 1, delete "50" and insert therefor --47--.

108. (Amended) A method for inserting data into digital data, the [device] method comprising the steps of:
storing an identifier corresponding to each of at least one user of a device which creates the digital data;

63
recognizing a user of the device whose identifier is stored in the memory;

outputting the identifier corresponding to the recognized user from the memory; and

inserting data corresponding to the identifier into the digital data.

--117. (New) A method for inserting a digital signature into digital data, the digital data comprising bits, the method comprising the steps of:

assigning predetermined bits of the digital data for receiving the digital signature;

inserting associated data into the digital data;

signing the digital data excluding the predetermined bits resulting in the digital signature; and

64
inserting the digital signature into the predetermined bits of the digital data for subsequent authentication of the digital data and associated data;

wherein the associated data comprises at least two fields.

118. (New) The method of claim 117, wherein at least one of the fields comprises data identifying a public key needed to decrypt the digital signature.

119. (New) The method of claim 118, wherein at least one other field comprises data identifying the owner of the public key.

120. (New) A method for inserting a digital signature into digital data, the digital data comprising bits, the method comprising the steps of:

assigning predetermined bits of the digital data for receiving the digital signature;

receiving associated data from a Global Positioning Satellite transmission;

inserting the associated data into the digital data;

signing the digital data excluding the predetermined bits resulting in the digital signature; and

inserting the digital signature into the predetermined bits of the digital data for subsequent authentication of the digital data and associated data.

121. (New) A method for inserting a digital signature into digital data, the digital data comprising bits, the method comprising the steps of:

assigning predetermined bits of the digital data for receiving the digital signature;

signing the digital data excluding the predetermined bits resulting in the digital signature;

inserting the digital signature into the predetermined bits of the digital data for subsequent authentication of the digital data;

providing time data identifying the time the digital data was created;

concatenating the hash and the time data;

applying a one-way hashing function to the concatenated hash and time data resulting in a second hash;

encrypting the second hash instead of the first hash to result in a time stamp containing the digital signature, wherein both the digital data and the time data are subsequently authenticated;

transmitting the hash and signature to a third party for performance of the providing, concatenating, and encrypting steps; and

receiving the time stamp from the third party prior to the inserting step;

wherein the trusted third party resides at an internet address and the transmitting and receiving steps are done through the internet.

B6
122. (New) A method for inserting a digital signature into digital data, the digital data comprising bits, the method comprising the steps of:

assigning predetermined bits of the digital data for receiving the digital signature;

inserting associated data into the digital data;
signing the digital data excluding the predetermined bits resulting in the digital signature; and
inserting the digital signature into the predetermined bits of the digital data for subsequent authentication of the digital data and associated data;
storing an identifier in a memory corresponding to each of at least one user of a device which creates the digital data;
recognizing a user of the device whose identifier is stored in the memory; and
outputting the identifier corresponding to the recognized user from the memory to be inserted as the associated data.

123. (New) The method of claim 122, wherein the recognizing step is accomplished by a fingerprint recognition system.

124. (New) An encoder for inserting a digital signature into digital data, the digital data comprising bits, the encoder comprising:

means for assigning predetermined bits of the digital data for receiving the digital signature;

means for inserting associated data into the digital data prior to signing the digital data, the associated data comprising at least two fields;

means for signing the digital data excluding the predetermined bits resulting in the digital signature; and

means for inserting the digital signature into the predetermined bits of the digital data for subsequent authentication of the digital data and the associated data.

125. (New) The encoder of claim 124, wherein at least one of the fields comprises data identifying a public key needed to decrypt the digital signature.

126. (New) The encoder of claim 125, wherein at least one other field comprises data identifying the owner of the public key.

127. (New) An encoder for inserting a digital signature into digital data, the digital data comprising bits, the encoder comprising:

means for assigning predetermined bits of the digital data for receiving the digital signature;

means for receiving associated data from a Global Positioning Satellite transmission, the associated data comprising data identifying the identity of an owner of the digital data;

means for inserting the associated data into the digital data prior to signing the digital data;

means for signing the digital data excluding the predetermined bits resulting in the digital signature; and

means for inserting the digital signature into the predetermined bits of the digital data for subsequent authentication of the digital data and the associated data.

128. (New) An encoder for inserting a digital signature into digital data, the digital data comprising bits, the encoder comprising:

means for assigning predetermined bits of the digital data for receiving the digital signature;

means for inserting associated data into the digital data prior to signing the digital data;

means for signing the digital data excluding the predetermined bits resulting in the digital signature;

means for inserting the digital signature into the predetermined bits of the digital data for subsequent authentication of the digital data and the associated data;

means for providing time data identifying the time the digital data was created;

means for concatenating the hash and the time data;

means for applying a one-way hashing function to the concatenated hash and time data resulting in a second hash;

means for encrypting the second hash instead of the first hash to result in a time stamp containing the digital signature, wherein both the digital data and the time data are subsequently authenticated;

means for transmitting the hash to a third party for providing the time stamp and concatenating the hash and time stamp; and

means for receiving the second hash from the third party prior to encryption;

wherein the trusted third party resides at an internet address and the means for transmitting and receiving is a computer capable of accessing the internet and receiving the transmitted second hash.

129. (New) An encoder for inserting a digital signature into digital data, the digital data comprising bits, the encoder comprising:

means for assigning predetermined bits of the digital data for receiving the digital signature;

a memory for storing an identifier corresponding to each of at least one user of a device which creates the digital data;

recognition means for recognizing a user of the device whose identifier is stored in the memory, wherein the recognition means is a fingerprint recognition system;

output means for outputting the identifier corresponding to the recognized user from the memory to be inserted as associated data

means for inserting the associated data into the digital data prior to signing the digital data;

means for signing the digital data excluding the predetermined bits resulting in the digital signature; and

means for inserting the digital signature into the predetermined bits of the digital data for subsequent authentication of the digital data and the associated data;

130. (New) A method for inserting data into digital data for subsequent authentication of the digital data, the method comprising the steps of:

receiving data from a radio frequency transmission;
inserting the data into the digital data; and
authenticating the digital data.

131. (New) A method for inserting data into digital data for subsequent authentication of the digital data, the method comprising the steps of:

receiving data from an internet link;
inserting the data into the digital data; and
authenticating the digital data.

132. (New) A device for inserting data into a digital data for subsequent authentication of the digital data, the device comprising:

an antenna for receiving data from a radio frequency transmission;

means for inserting the data into the digital image; and

means for authenticating the digital data.

133. (New) A device for inserting data into a digital image for subsequent authentication of the digital image, the device comprising:

a computer capable of accessing the internet and receiving data from an internet link;

means for inserting the data into the digital image; and

means for authenticating the digital image.

134. (New) A device for inserting data into digital data, the device comprising:

a memory for storing an identifier corresponding to each of at least one user of the device;

a fingerprint recognition means for recognizing a user of the device whose identifier is stored in the memory;

means for outputting the identifier corresponding to the recognized user from the memory; and